DIGITAL HANDBOOK CYBERSECURITY

An immediate reference for non tech-savvy users.

User Account & Passwords

DOs	DONTs
Set up complex passwords which is easy to remember, but hard for others to guess and crack.	NEVER EVER set the same passwords for different website.
Change passwords every 2-3 months.	NEVER EVER share your passwords even with your closest friends, teachers, external people.
After your activity, remember to log out from the website/app.	NEVER use your personal data as part of your password.

Social Media & Online Communication

DOs	DONTs
Think before you send a message, go live, or upload a post to the public.	NEVER EVER send any message that may insult, threaten, or leak the religion, caste, or any other sensitive information of any person.
Always report to your parents or any trusted adult if you are getting unwanted or dangerous posts or threats.	NEVER EVER accept a friend invite from a stranger.
Use pseudonymised names which hide your true identity.	NEVER reveal your true identity in public.

Device Security

DOs	DONTs
Set up a wireless secure router before connecting to it. The Wi-Fi should be privately visible to you and your devices ONLY.	NEVER EVER connect to public Wi-Fi offered in shopping malls. They can view and store data from your device.
Download anti-malware and anti-virus software which will protect you and your device from unsafe websites and applications.	NEVER EVER leave your device unattended. If you have to, lock it or shut it down .
Set passwords which include an uppercase and lowercase letter(s), numbers, symbols, etc.	NEVER enter your device’s password when someone is looking at your device.